

REMARKS

By this amendment, claims 1-32 are pending, in which claims 1, 5, 8, 9, 16, 22, 24, 25, 27, 28, and 30 are currently amended, claims 31 and 32 are newly presented, and no claims are canceled or withdrawn from consideration. No new matter is introduced.

The Office Action mailed November 21, 2003 rejected claims 25-27 and 28-30 under 35 U.S.C. § 112, ¶ 2 as being indefinite, claims 1, 5-7, 9, and 13-15 under 35 U.S.C. § 103(a) as obvious over *Ji et al.* (U.S. 5,623,600) in view of *Shanklin et al.* (U.S. 6,578,147), and claims 2-4, 10-12, and 16-30 under 35 U.S.C. § 103(a) as obvious over *Ji et al.* in view of *Shanklin et al.* and further in view of *Wells* (U.S. 6,338,141).

Regarding the indefiniteness rejections, claims 25 and 28 have now been amended to remove the antecedent basis issues pointed to by the Office Action. Applicants therefore respectfully request that these rejections be withdrawn.

Applicants respectfully traverse the rejections under 35 U.S.C. § 103, in that none of *Ji et al.*, *Shanklin et al.*, nor *Wells*, singly or in combination, discloses the claimed features.

For example, independent claims 1, 8, 9, and 16, as amended, each include the feature “**distributing a copy of the flow** to each of the scanning computer systems in parallel.” Independent claims 17, 18, and 19 each recite “**duplicating the flow** to produce a plurality of copies of the flow.” Independent claims 20 and 21 each recite “receiving **respective copies of a flow of content** from the front-end processor in parallel.” Independent claims 22, 25, and 28 each include the feature “receiving an alarm ... when **a flow of content scanned by the scanning computer systems in parallel** contains malicious code, said flow including at least one of a hypertext markup file and a transferred file.”

In its rejection of claims 1 and 9, the Office Action, at Page 4, lines 5-6, correctly acknowledges, "It fails to teach 'a plurality of scanning computer systems' and distributing 'copies of the flow to each of the scanning computer systems in parallel for scanning.'"

However, the Office Action, at Page 4, states:

Shanklin teaches that the internetworking device (i.e. a front end processor) inspects packets incoming from the external network and a load balancing unit implemented in the internetworking device performs a "copy to" operation [sic] **to send each packet to the sensors**, see col. 6, lines 25-46, where in a detection engine examines and analyses each packet and if the analysis indicates a misuse (or a malicious code), the sensor sends an alarm to a separate detection management station to take action (i.e. countermeasure), see col. 3, lines 55-65, see also col. 4, line 54 through col. 5, line 7.

Shanklin et al. (Per Abstract) is directed to a system for detecting unauthorized signatures to or from a local network. Multiple sensors, connected at an internetworking device, operate in parallel, and each receives **a portion of traffic** through the internetworking device, at a session-based level or at a lower (packet-based) level. At col. 6, lines 39-44 as cited by the Office Action, *Shanklin et al.* states, "Specifically, a 'copy to' operation is used to send **each packet to the appropriate sensor** as well as to the destination in local network 10 to which the packet is addressed. For example, router 21 may encapsulate the packet so that its new header information addresses the packet to **the appropriate sensor**." Thus, *Shanklin et al.* sends different packets to each of multiple processors, with each processor configured to perform processing that is identical to each other processor, but processing different packets in parallel.

This is discussed further at col. 2: 59 - col. 3: 3, wherein *Shanklin et al.* states:

Two specific embodiments of the invention are described herein. A first embodiment provides multiple sensors at the output of a router. A second embodiment provides multiple sensors inside a switch. In both cases, **each sensor is identical to the other sensors and is capable of performing the same intrusion detection processing**. The sensors operate in parallel, and analyze packets to determine if any packet or series of packets has a "signature" that matches one of a collection of known intrusion signatures. Thus, the invention

provides an easily scalable solution to providing an intrusion detection system whose ability to perform signature analysis can keep up with high speed networks.

Further, at col. 5: 21-28, *Shanklin et al.* states:

In the embodiment of FIG. 2, the load balancing is "session-based", which means that each sensor 21 handles a portion of the sessions incoming to the network. A stream of packets, S1, S2, . . . S6, . . . is illustrated. In the example of FIG. 2, the load balancing is such that **S1 goes to a first sensor, S2 to a second, S3 to a third, S4 to the first, and so on.** Thus, each sensor 21 handles one-third of the sessions in a given datastream.

At col. 5: 56-62, *Shanklin et al.* states:

FIG. 3 illustrates an alternative intrusion detection system 30, also having a router 32 and parallel sensors 31, but where the load balancing is "packet-based". Router 32 has a load balancing unit 32a, which distributes a packet stream comprised of packets P1, P2, . . . P6 The load balancing is such that **P1 goes to a first sensor, P2 to a second, P3 to a third, P4 to the first, and so on.**

Thus, each sensor of *Shanklin et al.* is identical to the other sensors, and each is performing the same intrusion detection process, providing an easily scalable solution. Each of the sensors receives sessions or packets (depending on the embodiment as shown in *Shanklin et al.*) that are different from the sessions or packets received by the other sensors.

In stark contrast, each of claims 1 and 9, as amended, recites "distributing **a copy** of the flow **to each of the scanning computer systems in parallel for scanning.**" This feature, as recited by either of claims 1 or 9, is neither suggested by *Ji et al.* nor *Shanklin et al.* singly, nor by any reasonable combination thereof. Therefore, Applicants respectfully request the withdrawal of the rejection of claims 1 and 9.

The rejection of dependent claims 5-7 and 13-15 should be withdrawn for at least the same reasons as those discussed above with regard to their respective independent claims, and these claims are separately patentable on their own merits.

Attention is now directed to the obviousness rejection of claims 2-4, 10-12, and 16-30 over *Ji et al.* in view of *Shanklin et al.* and further in view of *Wells*.

Wells (Per Abstract) is directed to the detection of computer viruses in computer files by using a collection of "relational data." The collection of relational data comprises various relational signature objects created from viruses. There is no mention whatever of distributing anything to scanning computer systems "**in parallel.**" Thus, *Wells* fails to fill in the gaps of *Ji et al.* in view of *Shanklin et al.* discussed above with regard to claims 1 and 9. Therefore, the obviousness rejection of claims 2-4 and 10-12, which depend from claims 1 and 9, respectively, should be withdrawn, as these claims depend from allowable independent claims, and as these claims are separately patentable on their own merits.

Regarding claim 8, the Office Action, at Page 7, lines 7-8, asserts, "Claim 8 is an apparatus corresponding to method claims 1-7. Claim 8 is rejected for the same reasons states [sic] in the rejections of claims 1-7 above." However, the Office Action does not specify which references are used to reject claim 8 (see Office Action, page 3, line 1 and page 6, line 8), nor how it is rejected.

In any event, Applicants respectfully request the withdrawal of the rejection of claim 8 as reciting, at least, "distributing **a copy of the flow** to each of the scanning computer systems in parallel for scanning," which, as discussed previously, is neither suggested nor disclosed by any of the applied references, neither singly nor by any reasonable combination thereof. Additionally, Applicants respectfully submit that none of claims 1-7 recites a method "corresponding to" apparatus claim 8, as asserted by the Office Action. However, if a next Office Action maintains the rejection of claim 8, Applicants respectfully request that the next Office Action be made non-final, as the reasoning asserted by the current rejection of claim 8 contravenes 35 U.S.C. § 132, which requires the Director to "notify the applicant thereof, stating

the reasons for such rejection.” This section is violated if the rejection “is so uninformative that it prevents the applicant from recognizing and seeking to counter the grounds for rejection.” *Chester v. Miller*, 15 USPQ2d 1333 (Fed. Cir. 1990). This policy is captured in the Manual of Patent Examining Procedure. For example, MPEP § 706 states that “[t]he goal of examination is to clearly articulate any rejection early in the prosecution process so that applicant has the opportunity to provide evidence of patentability and otherwise respond completely at the earliest opportunity.” Furthermore, MPEP § 706.02(j) indicates that: “[i]t is important for an examiner to properly communicate the basis for a rejection so that the issues can be identified early and the applicant can be given fair opportunity to respond.”

Applicants additionally submit that claim 8 recites “a plurality of scanning computer systems configured to execute respective anti-virus software having different, corresponding coverage of malicious code for scanning content for malicious code.” As pointed out previously, each sensor of *Shanklin et al.* is identical to the other sensors, and each is performing the same intrusion detection process. Applicants note that, in its rejection of claim 5, the Office Action, at page 5, lines 3-11, asserts, “Ji’s gateway includes FTP proxy server and a SMTP proxy server executed concurrently in a manner such that viruses transmitted to or from the network in messages and files are detected ... and that the routines (i.e. scanning software for detecting viruses (i.e. malicious codes) in the file transfers and the messages primarily include the FTP proxy server and the SMTP proxy server ... The teachings of JI clearly suggests that the gateway includes a scanning computer system configured to execute anti-virus routines having different, corresponding coverage of malicious code. That is, viruses carried by **file transfers and by messages** through **respective** FTP and SMTP proxy servers.”

There is no mention at all of any motivation for “distributing **a copy of the flow** to each of the scanning computer systems in parallel for scanning.” Assuming, arguendo, that the FTP

proxy server and the SMTP proxy servers were equated with the recited “each of the scanning computer systems,” then a “copy of the flow” would be distributed to the FTP proxy server and the SMTP proxy server. However, *Ji et al.* (per Abstract) clearly states, “The FTP proxy server and the SMTP proxy server scan all incoming and outgoing **files and messages, respectively** before transfer for viruses and then transfer the files and messages, only if they do not contain any viruses. Thus, *Ji et al.* teaches **away** from the recited “distributing a **copy of the flow to each** of the scanning computer systems **in parallel** for scanning,” as the FTP proxy server of *Ji et al.* scans files and the SMTP proxy server scans messages, and thus there is no suggestion or mention of the features recited by claim 8 in either of *Ji et al.*, *Shanklin et al.*, singly, or any reasonable combination thereof.

Regarding independent claim 16, the Office Action, at Page 7, lines 9-10, asserts, “Claim 16 is a method claim reciting limitations of claims 1-3, 5-7. Claim 16 is rejected for the same reasons states [sic] in the rejections of claims 1-3, 5-7 above.”

Applicants respectfully request the withdrawal of the rejection of claim 16 as reciting, at least, “distributing a **copy of the flow** to the scanning computer systems in parallel,” a feature which is neither suggested nor disclosed by any of the applied references singly nor in any reasonable combination, as discussed previously. Additionally, Applicants respectfully submit that an assertion by the Office Action that claim 16 “is a method claim reciting limitations of claims 1-3, 5-7” forces Applicants to pick and choose among features recited by other claims, and to conjecture how the applied references might somehow suggest or disclose claim 16. Therefore, if a next Office Action maintains the rejection of claim 16, Applicants respectfully request that the next Office Action be made non-final, as the reasoning asserted by the current rejection of claim 16 contravenes 35 U.S.C. § 132, as discussed above.

Regarding the rejection of claims 17-19, the Office Action, at Page 7, lines 11-12, asserts, "Claims 17-19 are apparatus, method and a computer-readable medium claims reciting limitations of claims 1 and 6. Claims 17-19 are rejected as such." However, each of independent claims 17, 18, and 19 recite, at least, "duplicating **the flow** to produce a plurality of copies of **the flow**," and "distributing the copies of **the flow** to **each of the scanning computer systems in parallel**" which is neither explicitly recited by either of claims 1 or 6, nor which is addressed anywhere in the Office Action. Further, Applicants respectfully submit that these features, as recited by each of claims 17, 18, and 19, is neither suggested nor disclosed by any of the applied references, neither singly nor by any reasonable combination thereof. Therefore, Applicants respectfully request the withdrawal of the rejection of claims 17-19. Additionally, if a next Office Action maintains the rejection of these claims, Applicants respectfully request that the next Office Action be made non-final, as the reasoning asserted by the current rejection of claims 17-19 contravenes 35 U.S.C. § 132, as discussed above.

Regarding the rejection of claim 20, the Office Action, at Page 7, lines 13-14, asserts, "Claim 20 is an apparatus claim reciting limitations of claims 1 and 6. Claim 20 is rejected for the same reasons provided in the statement of rejections of claims 1 and 6 above." However, claim 20 recites, at least, "executing respective anti-virus scanning software ..." which is not explicitly recited by either of claims 1 or 6, and which is neither suggested nor disclosed by any of the applied references, neither singly nor by any reasonable combination thereof. By not addressing these features, Applicants are again left to rely on conjecture for the Office Action's reasoning, in contravention of 35 U.S.C. § 132, as discussed previously. However, Applicants respectfully request the withdrawal of the rejection of claim 20, as Applicants respectfully submit that claim 20 is neither suggested nor disclosed by any of the applied references, neither singly nor by any reasonable combination thereof. Additionally, if a next Office Action maintains the

rejection of this claims, Applicants respectfully request that the next Office Action be made non-final, as the reasoning asserted by the current rejection of claim 20 contravenes 35 U.S.C. § 132, as discussed above.

Regarding the rejection of claim 21, the Office Action, at Page 7, lines 15-16, asserts, "Claim 21 is method claim **reciting limitations of claims 1, 5 and 6**. Claim 21 is rejected for the same reasons provided in the statement of rejections of claims 1, 5 and 6 above." However, claim 21 recites, at least, "receiving respective **copies of a flow of content** from the front-end processor in parallel ..." which is not explicitly recited by any of claims 1, 5 or 6, and which is neither suggested nor disclosed by any of the applied references, neither singly nor by any reasonable combination thereof. By not addressing these features, Applicants are again left to rely on conjecture for the Office Action's reasoning, in contravention of 35 U.S.C. § 132, as discussed previously. However, Applicants respectfully request the withdrawal of the rejection of claim 21, as Applicants respectfully submit that claim 21 is neither suggested nor disclosed by any of the applied references, neither singly nor by any reasonable combination thereof. Additionally, if a next Office Action maintains the rejection of claim 21, Applicants respectfully request that the next Office Action be made non-final, as the reasoning asserted by the current rejection of claim 21 contravenes 35 U.S.C. § 132, as discussed above.

Regarding the rejection of claims 22-23 and 24, the Office Action, at Page 7, lines 17-20, asserts, "Claims 22-23 are apparatuses **implementing features of claims 1, 6 and 7**. Claim 22 is rejected as such," and "Claim 24 is an apparatus corresponding to method claims 1, 2, and 4. Claim 24 is rejected as such." Again, the rejection of these claims is so vague that Applicants are left to rely on conjecture for the Office Action's reasoning, in contravention of 35 U.S.C. § 132, as discussed previously. However, Applicants submit that claim 22 recites "**a flow of content** scanned by the scanning computer systems in parallel," and claims 23 and 24 depend from claim

22. Again, Applicants respectfully request the withdrawal of the rejection of claims 22-23 and 24, as Applicants respectfully submit that claims 22, 23 and 24 are neither suggested nor disclosed by any of the applied references, neither singly nor by any reasonable combination thereof. Additionally, if a next Office Action maintains the rejection of these claims, Applicants respectfully request that the next Office Action be made non-final, as the reasoning asserted by the current rejection of claims 22, 23, and 24 contravenes 35 U.S.C. § 132, as discussed above.

Regarding the rejection of claims 25-27 and 28-30, the Office Action, at Page 7, line 21-Page 8, line 3, asserts, "Claims 25-27 **recite limitations of claims 1, 2, 4, 6 and 7**. Claims 25-27 are rejected for the same reasons provided in the statement of rejections of claims 1, 2, 4, 6 and 7 above," and "Claims 28-30 are apparatuses **implementing limitations of claims 1-4, 6 and 7**. Claims 28-30 are rejected for the same reasons provided in the statement of rejections of claims 1-4 and 6-7." Again, the rejection of these claims is so vague that Applicants are left to rely on conjecture for the Office Action's reasoning, in contravention of 35 U.S.C. § 132, as discussed previously. However, each of these claims recites, at least, "**a flow of content** scanned by the scanning computer systems in parallel." Again, Applicants respectfully request the withdrawal of the rejection of claims 25-27 and 28-30, as Applicants respectfully submit that claims 25-27 and 28-30 are neither suggested nor disclosed by any of the applied references, neither singly nor by any reasonable combination thereof. Additionally, Applicants respectfully submit that an assertion by the Office Action, e.g., that claims 25-27 "**recite limitations of claims 1, 2, 4, 6 and 7**" forces Applicants again to pick and choose among features recited by other claims, and to conjecture how the applied references might somehow suggest or disclose claims 25-27. Therefore, if a next Office Action maintains the rejection of claims 25-27 and 28-30, Applicants respectfully request that the next Office Action be made non-final, as the reasoning asserted by the current rejection of claims 25-27 and 28-30 contravenes 35 U.S.C. § 132, as discussed above.

New dependent claim 31, which depends from claim 1, recites “wherein each one of the plurality of scanning computer systems is configured to execute malicious code detection software other than detection software executed by any other one of the plurality of scanning computer systems.” New dependent claim 32, which depends from claim 1, recites “wherein said scanning at each of the scanning computer systems includes executing malicious code detection software other than detection software executed by any other one of the plurality of scanning computer systems.” (See, e.g., specification, page 3, ¶ 10, page 8, ¶ 25, and page 9, ¶ 29). Each of these claims is allowable for at least the same reasons as its respective independent claim and each is separately patentable on its own merits.

Therefore, the present application, as amended, overcomes the objections and rejections of record and is in condition for allowance. Favorable consideration is respectfully requested. If any unresolved issues remain, it is respectfully requested that the Examiner telephone the undersigned attorney at 703-425-6499 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

DITTHAVONG & CARLSON, P.C.

2/23/04
Date

Margo Livesay
Margo Livesay, Ph.D.
Reg. No. 41,946

Phouphanomketh Ditthavong
Reg. No. 44,658

Attorneys for Applicant(s)

10507 Braddock Road
Suite A
Fairfax, VA 22032
Tel. 703-425-6499
Fax. 703-425-8518